In the Claims:

1.(presently amended) A N-dimensional biometric security system comprising

a station for receiving input information from a user representative of the user and generating a ~~responsive~~ signal responsive thereto;

a first data base having a plurality of words and language rules for generating one-time challenge phrases corresponding to the user and a session access request ~~therein~~;

a second data base having biometric models of the ~~users~~ user therein; and

a controller to receive and validate said signal as representative of the user, said controller communicating with said first data base for delivering a randomly generated challenge phrase at said station for the user to speak in response to validation of said signal, and said controller communicating with said station

to receive a spoken response and to generate a second signal representative of the spoken response,

to process said second signal by automatic speech recognition (ASR) for ASR matching to validate the the voice information used for speaker recognition and to issue a first validation signal in repsonse to matching and

to process said second signal to verify the voice information used for speech recognition and to issue a second validation signal in repsonse to matching

to validate ~~a~~ the spoken response to said selected challenge phrase as representative of the user in response to receiving said first validation signal and said second validation signal.

2.(presently amended) A method of identifying and validating a user comprising the steps of

~~having a user~~ initially ~~input~~ inputting information representative of the user at a station;

generating a signal responsive to the information;

receiving and validating the signal as representative of the user;

thereafter delivering a randomly generated challenge phrase at said station for the user to speak in response to validation of said signal;

~~having said user speak the randomly generated challenge phrase and~~ generating a second signal representative of the spoken response to said challenge phrase; and

thereafter receiving and validating the second signal as representative of the user.

3. (new) An N-dimensional biometric security system comprising

a station for receiving input information from a user representative of the user and generating a first signal responsive thereo;

a first data base for storing a plurality of stored word phrases;

a second data base for storing a biometric model of the user; and

a controller for receiving and comparing said first signal to the stored biometric model and for validating said first signal as representative of the user in response to a match between said first signal and said stored biometric model, said controller being operatively connected to said first data base to randomly select and forward one of said stored word phrases in response to said first signal to said station as a challenge phrase for the user to speak, said controller communicating with said station to receive and compare a spoken response to said challenge phrase to said challenge phrase to verify said spoken response as matching said challenge phrase and to compare at least part of said spoken response to the stored biometric model and for validating said spoken response as representative of the user in response to a match between said spoken response and said stored biometric model, said controller issuing an authentication signal in response to a verification of said spoken response as matching said challenge phrase and a validation of said spoken response as representative of the user.

4. (new) A N-dimensional biometric security system comprising

a station for receiving input information from a user representative of the user and generating a first signal responsive thereo;

a first data base for storing a plurality of stored word phrases;

a second data base for storing a biometric model of each of a multiplicity of users; and

a controller for receiving and comparing said first signal to the stored biometric model and for validating said first signal as representative of the user in response to a match between said first signal and said stored biometric model, said controller being operatively connected to said first data base to randomly select and forward one of said stored word phrases in response to said first signal to said station as a challenge phrase for the user to speak, said controller communicating with said station to receive and compare a spoken response to said challenge phrase to said challenge phrase to verify said spoken response as matching said challenge phrase and to compare at least part of said spoken response to the stored biometric models and for validating said spoken response as representative of the user in response to a match between said spoken response and said stored biometric model of the user, said controller issuing an authentication signal in response to a verification of said spoken response as matching said challenge phrase and a validation of said spoken response as representative of the user.

5. (new) A method of identifying and validating a user comprising the steps of

receiving information from a user representative of the user at an input station and generating a first signal responsive thereo;

storing a plurality of stored word phrases in a first data base;

storing a biometric model of each of a multiplicity of users in a second data base;

receiving and comparing said first signal to the stored biometric models to validate said first signal as representative of one of said users in response to a match between said first signal and said stored biometric models;

randomly selecting and forwarding one of said stored word phrases in response to said first signal to said station as a challenge phrase for the user to speak;

comparing a spoken response to said challenge phrase to verify said spoken response as matching said challenge phrase;

comparing at least part of said spoken response to the stored biometric models for validating said spoken response as representative of said one of said users in response to a match between said spoken response and said stored biometric model of said one user; and

issuing an authentication signal in response to a verification of said spoken response as matching said challenge phrase and a validation of said spoken response as representative of said one user.

6. (new) A method as set forth in claim 5 wherein the user randomly selects one of said stored word phrases as said challenge phrase.